

REMARKS

Claims 1-17, 19-24, 26-29, 31-38 and 41-44 are rejected.

Claim Rejections – 35 USC § 102(b)

The Patent Office rejected claims 1-4, 6-12, 14-15, 17, 19-20, 22, 23, 27-29, 31-38, and 41-40 under 35 U.S.C. 102(b) as being anticipated by Nolet (U.S. Pat. 6,138,249). The applicant includes the following comments to clearly distinguish the claimed invention over the art cited by the Examiner, and respectfully requests a favorable reconsideration of claims 1-4, 6-12, 14-15, 17, 19-20, 22, 23, 27-29, 31-38, and 41-40.

For a claim to be anticipated, each and every non-inherent limitation must be disclosed in a single reference (MPEP 2131).

Regarding the Examiner's rejections of the Applicant's independent claims 1, 9, 17, 29, 34, and 41 and dependent claims 2-4, 6-8, 10-12, 14-15, 19-20, 22, 23, 27-28, 31-33, 35-38, and 40, the Applicant respectfully requests reconsideration in light of the discussion below.

Exemplary embodiments of the disclosed invention address and solve the problems detailed in paragraph [0006] where disk drive manufacturers would “typically receive predictive failure analysis information from disk drives that have been called out for replacement on a per device basis, but **recovered error information** is not typically received from the drives that are functioning within their tolerances”. Furthermore, a “point may arrive at which the unrecovered error rate becomes unacceptably high, or the number or severity of the recovered errors may become **symptomatic of an impending total failure. Predictive failure analysis algorithms within the disk drive firmware are used to estimate this point and to generate alerts to users**, informing them that a service action should be scheduled to replace the **hardware which may be about to fail**” (see [0003]). In particular, Applicants have determined that it would be useful to have a system where a “software agent 50 gathers recovered error and other predictive statistical data from the disk drives 80” (see

[0025]). Then, **recovered “error information** is provided from a large population of drives in the field population, and may be used to perform detailed analysis with greater predictability and less tolerance than present arrangements”. Trends or unexpected failure modes may also be detected” (see [0041]). When the “data reaches the manufacturers server it is processed (block 330) and the results may be used for ... **new microcode with improved error recovery**” and/or “which is **more tolerant of certain error events** than the original drive microcode and which will not call for unnecessary early drive replacement, where it has been established that the original algorithm was too aggressive, thus reducing service cost” (see [0035] and [0036]). In addition to providing important information “the new microcode may be available” so that “the predictive failure analysis algorithms of each disk drive in the field may be continually improved rather than being fixed from the date of manufacture.” (see [0037]). (Emphasis added throughout.)

Claim 1 recites:

“A server for improving predictive failure attributes of distributed devices, comprising:

a receiver for receiving, via a network, failure analysis data from individual ones of a plurality of distributed devices; where

each device of said plurality of distributed devices comprises failure analysis software comprising a **predictive failure analysis algorithm** arranged for collecting failure analysis data of said distributed device and a communications device arranged for transmitting said failure analysis data to said network;

wherein said server is arranged for analyzing said failure analysis data and for providing in response to the analysis an updated **predictive failure analysis algorithm** to the plurality of distributed devices , wherein each of said plurality of distributed devices is coupled to said network, wherein the **updated predictive failure analysis algorithm** is provided to the plurality of distributed devices in the form of a first microcode that is provided from the server to be used instead of a second microcode previously used by the plurality of distributed devices, wherein the **first microcode and the second microcode have different tolerances of certain error events**” (emphasis added).

The Examiner states Nolet teaches:

“a server for improving predictive failure attributes of distributed devices

(column 7, lines 55-58; column 8, line 57), comprising: a receiver for receiving, via a network, failure analysis data from individual ones of a plurality of distributed devices (column 7, lines 55-60); where each device of said plurality of distributed devices comprises failure analysis software comprising a predictive failure analysis algorithm arranged for collecting failure analysis data of said distributed device (column 8, lines 29-48, wherein each device has a software agent that tests/monitors the device and transmits that information; column 1, lines 62 – column 2, line 8, wherein, the collected data at the distributed devices can be used for predicting future problems in the manufacturing process); and a communications device arranged for transmitting said failure analysis data to said network (column 5, lines 18-29; column 8, lines 33-36; column 6, lines 48-67); wherein said server is arranged for analyzing said failure analysis data and for providing in response to the analysis an updated predictive failure analysis algorithm to the plurality of distributed devices, wherein each of said plurality of distributed devices is coupled to said network, wherein the updated predictive failure analysis algorithm is provided to the plurality of distributed devices in the form of a first microcode that is provided from the server to be used instead of a second microcode previously used by the plurality of distributed devices, wherein the first microcode and the second microcode have different tolerances of certain error events (column 8, lines 57-59, 40-48; column 18, lines 1-4, wherein the central monitoring center gets the service requests from the devices and analyses the data to see which monitoring/testing software the device is currently running, if the currently used software is not the most up to date, the center transmits the most current updated software to the devices for the future monitoring of the devices; column 13, line 59 – column 14, line 9)” (page 2 and 3 of the Office Action dated March 27, 2007).

The Applicants respectfully assert the Examiner has misinterpreted the teachings in Nolet.

The disclosure in Nolet is addressed to collecting information regarding failures: for example, when “a **failure occurs** during the test process, it is desirable to maintain a record of how the failure was dispositioned” (see column 1, line 62); “if a **system fails** in the field” (see column 1, line 67 to column 2, line 1); “determine when any of the data processing systems **experiences a failure**” (column 5, lines 20-21); “indicates the **nature of the failure**” (column 7, lines 19-20); etc. In contrast, the Applicants invention is directed at least in part to a “**predictive failure analysis algorithm**” (Claim 1) which generates analyses based upon a number of sources, including specifically, “recovered error information” (see [0041]). (Emphasis added throughout).

Claim 1 recites in part:

“each device of said plurality of distributed devices comprises failure analysis software comprising a **predictive failure analysis algorithm** arranged for collecting failure analysis data of said distributed device and a communications device arranged for transmitting said failure analysis data to said network;

wherein said server is arranged for analyzing said failure analysis data and for providing in response to the analysis an updated **predictive failure analysis algorithm** to the plurality of distributed devices, wherein each of said plurality of distributed devices is coupled to said network, wherein the **updated predictive failure analysis algorithm** is provided to the plurality of distributed devices in the form of a first microcode that is provided from the server to be used instead of a second microcode previously used by the plurality of distributed devices, wherein the first microcode and the second microcode have different tolerances of certain error events” (emphasis added).

As Nolet is directed towards collecting information regarding a system that has failed, Nolet lacks to ability to predict a failure. There is no mention in Nolet of predicting an impending failure in any particular device. A word search of Nolet returns no results for “predict”, “predictive”, “statistic”, “warn” or “anticipate”.

The Examiner asserts “the collected data at the distributed devices can be used for predicting future problems in the manufacturing process” (page 2) and relies upon column 1, lines 62 – column 2, line 8 as supporting this statement. This section states:

“When a failure occurs during the test process, it is desirable to maintain a record of how the failure was dispositioned. This can be particularly important in the event that a system fails in the field. One goal of the manufacture/test process is to **ensure that all errors are detected before the system is shipped to the customer**. Thus, if a system fails in the field, it is desirable to determine why the testing process did not detect the error prior to shipping, and to **adapt the process so that it can detect similar failures in the future**. The maintenance of records indicating the manner in which all errors on a particular system were dispositioned can be extremely **helpful in determining why a particular failure in the field was not detected** during the manufacture/test process” (emphasis added).

The Applicants assert that the Examiner has misinterpreted this section. The collected data is not used to “predict future problems”, but rather “in determining why a particular failure in the field was not detected”. Thus the information is not used for any prediction, but rather to “adapt the process so that it can detect similar failures in the future”. Even if this section disclosed the functionality

described by the Examiner, which the Applicants do not assert it does, “predicting future problems in the manufacturing process” does not disclose or suggest a “predictive failure analysis algorithms” (Claim 1).

In the Response to Arguments section of the Office Action dated March 27, 2007, the Examiner states: “the examiner reads the claim language definition of the predictive failure analysis algorithm to merely be a module arranged to collect failure analysis data of the device”. The interpretation used by the Examiner, as merely a module to collect data, lacks any predictive or warning features; it does not fully describe the limitation. For at least this reason alone, Nolet does not disclose or suggest “failure analysis software comprising a **predictive failure analysis algorithm** arranged for collecting failure analysis data of said distributed device” (emphasis added).

The Examiner asserts that Nolet discloses:

“the central monitoring center gets the service requests from the devices and analyses the data to see which monitoring/testing software the device is currently running, if the currently used software is not the most up to date, the center transmits the most current updated software to the devices for the future monitoring of the devices”.

The Examiner cites column 8, lines 57-59, 40-48; column 18, lines 1-4; and column 13, line 59 – column 14, line 9 in support. The Applicants respectfully assert this is a misinterpretation of the disclosure in Nolet.

At column 8, lines 29-64

“To address the concern regarding inventory transactions or test file updates being missed as a result of the polling loop time ... the embodiment ... employs a transaction-based procedure. In particular, each of the systems 21, 23 being monitored detects situations wherein information should be **updated in the APC monitor** 25, and notifies the monitor 25. This is similar to the call home feature discussed above, except that the notification is transmitted over the network 27, rather than a modem/telephone line connection. Each of the monitored systems 21, 23 has an associated agent 29, 31. Each agent 29, 31 monitors the relevant files of its associated system 21, 23, and when any of those files is updated, the agent performs two functions. First, the agent broadcasts a service request to the APC monitor 25 over the network 27, indicating that there has been a change of a relevant file that the

APC monitor 25 should be aware of. Second, the agent stores or queues the updated information so that as the monitored system continues to operate, the queued information will not be lost if the relevant file is updated again, and **will be available to the APC monitor 25** when it services the request. The queuing of the information by the agent ensures that no relevant information will be lost, even if there is a delay (e.g., due to the network 27 going down) in the APC monitor 25 servicing the broadcast request. The transaction based procedure is also advantageous in that it results in real time updates of the information in the APC monitor 25.

“The APC monitor 25 includes at least one server 33 that is responsible for servicing the requests broadcast by the agents 29, 31 over the network 27. In a manner that is discussed in more detail below, the servers 33 handle the broadcast requests by reading the relevant information from the requesting agent 29, 31 over the network 27, and then **updating the database 35** with the new information provided by the agent” (emphasis added).

This database is described more fully at column 8, lines 10-15:

“the database used during the manufacture/test monitoring process is also **used to manage the inventory** of the parts and subcomponents (collectively "parts") used in the systems under test. The database is automatically updated to **maintain accurate information** regarding the parts in each system under test” (emphasis added).

This section describes the agent providing update information to the monitor. Specifically this procedure is used to address “loss of some test data due to the polling delay” (see column 8, lines 16-17). The ‘update’ is actually used to provide inventory data (such as which devices have failed), not microcode. Additionally, the database being updated is used to “maintain accurate information”. There is no disclosure or suggestion of the server being “arranged for analyzing” this data, such as seen in Claim 1.

In the Response to Arguments section of the Office Action dated March 27, 2007, the Examiner states: “the updated microcode is based upon the request sent from the device, and this request was originally sent from the device based upon a failure in the device (column 6, lines 58-60).”

The Applicants respectfully assert that the Examiner has misinterpreted the disclosure of Nolet. Nolet recites:

“The method comprises the steps of: (A) executing a plurality of tests on each of the plurality of data processing systems to test the functional operation of the plurality of data processing systems, each one of the plurality of tests generating a failure when one of the plurality of data processing systems does not properly execute the one of the plurality of tests; (B) when a failing one of the plurality of data processing systems experiences a failure, storing information in the failing one of the plurality of data processing systems identifying a nature of the failure, and **broadcasting a service request** from the failing one of the plurality of data processing systems to the monitoring system, **the service request indicating that the failure has occurred**; and (C) storing information in the monitoring system to record the failure in response to information provided by the failing one of the plurality of data processing systems” (column 6, lines 51-67, emphasis added).

This section of Nolet discloses a service request that “indicates that the failure has occurred”. Nolet also discloses “the plurality of data processing systems includes request means for transmitting a service request to the service center **requesting a check of whether a resource in the one of the plurality of data processing systems is up to date**” (column 6, lines 21-25, emphasis added). These appear to be separate service requests and are composed differently; one indicates a failure, the other requests a check of the resources.

Consider further in column 17, line 63 through column 18, line 4, Nolet discloses:

“the agent for the data processing system 113 can automatically and periodically send to the customer service site 115, over the network 27, **service requests that provide the revision numbers** of certain software loaded on the data processing system, and **query whether those revisions are up to date**. In response to those service requests, the customer service center 115 can automatically download any new revisions of software to the data processing system 113” (emphasis added).

These “service requests” are designed specifically to request up-to-date software. There is no indication of that the server analyzes ‘failure data’ such as described in Claim 1: “wherein said server is arranged for analyzing said failure analysis data and for providing in response to the analysis an updated **predictive failure analysis algorithm**” (emphasis added). As seen above, Nolet does not disclose a predictive failure analysis algorithm, and as such, Nolet can not disclose providing an updated version of such an algorithm. Clearly, this is not a server analyzing failure analysis data and “providing in response to the analysis

an updated predictive failure analysis algorithm” that has “different tolerances of certain error events “(Claim 1).

In column 13, line 59 through column 14, line 9, Nolet discloses:

“The **service provider can be selected in step 97 in any of a number of ways**, using either a very simple selection algorithm or a more complex one. For example, each server can be assigned a number that it can return in the message sent to the requesting agent, and the agent can simply select the highest or lowest number to select a particular service provider. However, in accordance with one embodiment ... a more complex selection algorithm is employed in an attempt to increase the efficiency of the system. In particular, each of the servers 33A-33N (FIG. 3) that responds to a service request can calculate a cost associated with responding to the request. A number of factors can be considered in determining the cost of servicing a request, including a number of service requests that the server may have queued up, available memory in the server, etc. **Each server can then respond to the requesting agent with its cost information, and the agent can select the responding server with the lowest cost to handle the request**” (emphasis added).

This section appears to describe a method for an agent to select a server in order to handle a service request. There is no indication of an “updated predictive failure analysis algorithm”, analysis of failure data, or “microcode”.

Clearly, these sections, as relied upon by the Examiner, do not disclose a server where:

“said server is arranged for analyzing said failure analysis data and for providing in response to the analysis an updated predictive failure analysis algorithm to the plurality of distributed devices, wherein each of said plurality of distributed devices is coupled to said network, wherein the updated predictive failure analysis algorithm is provided to the plurality of distributed devices in the form of a first microcode that is provided from the server to be used instead of a second microcode previously used by the plurality of distributed devices, wherein the first microcode and the second microcode have different tolerances of certain error events” (Claim 1, emphasis added).

As was noted above, Nolet is devoid of any express reference to “predict”, “predictive”, “statistic”, “warn” or “anticipate”. Therefore, Nolet is devoid of a “predictive failure analysis algorithm” as in Claim 1. As Nolet does not disclose each and every non-inherent limitation of Claim 1, Nolet cannot anticipate Claim 1. Thus, Claim 1 is in a condition for allowance.

Independent claims 9, 17, 29, 34, and 41 share many similarities with claim 1; therefore, many of the above arguments apply to these claims as well.

Claim 9 recites:

“A device comprising:
a **predictive failure analysis algorithm** arranged for collecting failure analysis data of said device; and,
a communications device coupled to said predictive failure analysis algorithm arranged for **transmitting said failure analysis data** to a remote server via a network,
wherein said remote server is **arranged for analyzing said failure analysis data** received from said device and from other devices and for **providing an updated predictive failure analysis algorithm** to the device and the other devices, wherein the updated predictive failure analysis algorithm is provided to the device in the form of a first microcode that is provided from the remote server to be used instead of a second microcode previously used by the device and the other devices, wherein the **first microcode and the second microcode have different tolerances of certain error events**” (emphasis added).

Claim 17 recites:

“A method for performing predictive data analysis using a central server, said method comprising:
collecting failure analysis data in individual ones of a plurality of distributed devices in which **each of the distributed devices uses a predictive failure analysis algorithm**;
receiving said failure analysis data at the central server from a network coupled to each device of said plurality of distributed devices; **analyzing said failure analysis data** received from said each device at the central server; and
in response to the analysis, providing an updated predictive failure analysis algorithm from the central server to the distributed devices, wherein the updated predictive failure analysis algorithm is provided to the plurality of distributed devices in the form of a first microcode that is provided from the central server to the plurality of devices to be used instead of a second microcode previously used by the plurality of devices, wherein the **first microcode and the second microcode have different tolerances of certain error events**” (emphasis added).

Claim 29 recites:

“A computer program comprising computer readable program code stored on a

computer readable medium for performing failure analysis of a plurality of disk drives that comprise a part of at least one data storage system, comprising first program code for collecting failure analysis data from individual ones of said disk drives and for transmitting said collected failure analysis data to a central server via a network and second program code, executed at said central server, for analyzing said failure analysis data and **deriving an updated predictive failure analysis algorithm** therefrom, where **said updated predictive failure analysis algorithm is downloaded** to said plurality of disk drives via the network, wherein the updated predictive failure analysis algorithm is provided to the plurality of disk drives in the form of a first microcode from the central server to be used instead of a second microcode previously used by the plurality of disk drives, wherein the **first microcode and the second microcode have different tolerances of certain error events**” (emphasis added).

Claim 34 recites:

“A computer program comprising computer readable program code stored on a computer readable medium for performing failure analysis of a plurality of disk drives that comprise a part of at least one data storage system, comprising first program code, executed by a central server, for receiving, via a network, failure analysis data from said at least one data storage system for analyzing said failure analysis data and for **deriving an updated predictive failure analysis algorithm** therefrom, where **said updated predictive failure analysis algorithm is downloaded** to said plurality of disk drives via said network, wherein the updated predictive failure analysis algorithm is provided to the plurality of disk drives in the form of a first microcode to be used instead of a second microcode previously used by the plurality of disk drives, wherein the **first microcode and the second microcode have different tolerances of certain error events**” (emphasis added).

Claim 41 recites:

“A system for monitoring performance of a plurality of distributed devices via a network, comprising:

- a network;

- a central server having a monitoring capability, the central server being coupled to the network;

- a plurality of distributed devices which are coupled to the network and which are monitored by the central server via the network, each of the plurality of distributed devices having a failure data analysis capability **provided by a predictive failure analysis algorithm** of the corresponding distributed device, each of the plurality of distributed devices providing predictive failure data to the central server via the network, wherein the **central server modifies the predictive failure analysis**

algorithm in the form of a first microcode based on the predictive failure data to provide an updated predictive failure analysis algorithm in the form of a second microcode previously used by the plurality of distributed devices, wherein the **first microcode and the second microcode have different tolerances of certain error events**" (emphasis added).

Thus, Nolet does not anticipate independent claims 1, 9, 17, 29, 34, and 41. Claims 2-4, 6-8, 10-12, 14-15, 19-20, 22, 23, 27-28, 31-33, 35-38, and 40 are dependent claims and are allowable because their corresponding base claims are allowable.

In light of the discussion above, the Applicant respectfully asserts that a case for anticipation was not presented. As such, the Applicant respectfully requests that the Examiner reconsider and withdraw these rejections. However, in order to fully address the Examiner's rejections regarding dependent claims 2-4, 6-8, 10-12, 14-15, 19-20, 22, 23, 27-28, 31-33, 35-38, and 40, the Applicant submits the comments below.

Claim 7 recites:

"The server of claim 6 wherein said intermediary software agent is installed on a **local server**" (emphasis added).

Nolet does not show a local server on the same side of the network as the distributed devices, contrary to the Examiner's assertions regarding column 9, lines 57-59, of Nolet. Nolet discloses:

"In one embodiment ... shown in FIG. 3, **multiple servers are provided for fault tolerance reasons**. In FIG. 3, a plurality of servers 33A-33N is provided. Each of the servers includes at least one service. The **services that respond to service requests** broadcast over the network 27 by the agents 29, 31 (FIG. 2) can be implemented simply as a program, run on a PC or other device that implements the server, that is idle and awaits an appropriate broadcast request to initiate the program" (Column 9, lines 52-60, emphasis added).

Figure 3 of Nolet:

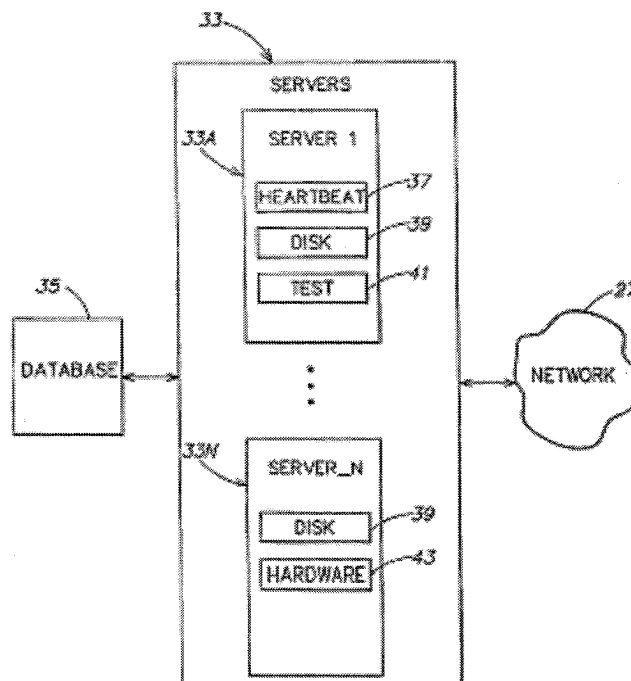


FIG. 3

Consider further:

“When each service is implemented on at least two servers, the fault tolerance of the system is improved because there is **no single point of failure** that would cause the APC monitor 25 (FIG. 2) to stop collecting information from the systems under test” (column 10, lines 13-17, emphasis added).

“wherein multiple ones of the servers 33A-33N implement the same service, a protocol is employed to determine **which of those servers will handle each service request** (column 10, lines 30-33)” (emphasis added).

The use of separate servers provides ‘fault tolerance’. All servers disclosed in Figure 3 of Nolet are located on the same side of the network and can communicate directly with the database without an intervening server. There is no indication that any of these servers operate as a host for an “intermediary software agent”.

In the Response to Arguments in the Office Action dated March 27, 2007, the Examiner states:

“Nolet teaches wherein the monitored device can a server [sic] (column 19, lines 26-29, so the monitoring agent of the monitored device is on a server device.”

This section (from column 19, lines 10-31) discloses:

“The process manager monitors information that enters the database in the monitor system (e.g., database 35 in FIG. 2), and reacts to it in a number of ways depending upon the nature of the information ... Another example of the process manager is the embodiment ... discussed above wherein software updates to the database can result in the process manager broadcasting information to the monitored systems to automatically update the software on those systems. In these situations, the central monitoring system acts more as a client, with the monitored systems **acting in a capacity that is generally viewed as that of a server**. The process manager or fourth tier provides a closed feedback loop system and bi-directional communication between the monitoring system and the systems being monitored” (emphasis added).

Here, Nolet is not describing a “local server”, but rather describing the actions of the agent as “acting in a capacity that is generally viewed as that of a server” since the “process manager broadcasting information to the monitored systems”. This does not disclose or suggest the use of a “local server” in any way, let alone a situation where an “intermediary software agent is installed on a local server” (Claim 7).

As Nolet does not disclose the “local server” of Claim 7, Nolet cannot anticipate Claim 7. Thus, Claim 7 is in a condition for allowance.

Dependent claims 8, 15, 22, and 23 share many similarities with claim 7; therefore, many of the above arguments apply to these claims as well.

Claim 8 recites:

“The server of claim 7, wherein said **local server** comprises a database arranged for storing said failure analysis data, said **local server** being arranged for periodically uploading said failure analysis data to said server” (emphasis added).

Claim 15 recites:

“The device of claim 14 wherein said intermediary software agent is installed on a **local server**” (emphasis added).

Claim 22 recites:

“The method of claim 17 wherein said each device is coupled to said network via an intermediary software agent installed on a **local server**” (emphasis added).

Claim 23 recites:

“The method of claim 22 wherein said intermediary software agent is installed on a **local server**” (emphasis added).

Claim Rejections – 35 USC § 103(a)

The Examiner has rejected the Applicant’s claims 5, 13, 16, 21, 24, 26 and 44 as being unpatentable under 35 U.S.C. 103(a) over Nolet in view of Ballard (U.S. Publ. Pat. No. 2003/0088538). The applicant includes the following comments to clearly distinguish the claimed invention over the art cited by the Examiner, and respectfully requests a favorable reconsideration of claims 5, 13, 16, 21, 24, 26 and 44.

The Examiner refers to a reference “Ballrd” (page 12). It is assumed the Examiner intended to refer to Ballard (U.S. Publ. Pat. No. 2003/0088538), but if this not the case, the Applicant requests the Examiner to provide detailed information regarding this reference.

It is well established law that in order for an obviousness rejection to be proper, the Patent Office must meet the burden of establishing a prima facie case for obviousness. Thus, as interpreted by the Courts, the Patent Office must meet the burden of establishing that all elements of the invention are disclosed in the prior art and that in accordance with *In re Lee*, the prior art must contain a suggestion, teaching, or motivation for one of ordinary skill in the art to modify a reference or combine references; and that the proposed modification must have had a reasonable expectation of success, determined from the vantage point of the skilled artisan at the time the invention was made.¹

¹ *In Re Fine* 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988); *In Re Wilson*, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970); *Agmen v. Chugai Pharmaceuticals Co.*, 927 U.S.P.Q.2d, 1016, 1023 (Fed. Cir. 1996); *In Re Sang Su Lee*, 277 F.3d 1338, 61 U.S.P.Q.2d 1430 (Fed. Cir. 2002).

Claim 5 recites:

“The server of claim 1, wherein said failure analysis data provides an indication of operating lifespan of said plurality of distributed devices.”

The Examiner states that “Nolet does not explicitly teach wherein said failure information provides an indication of operation lifespan” (page 11). On this point, the Applicants agree with the Examiner.

The Examiner asserts that Ballard teaches “failure information provides an indication of operation lifespan of said plurality of distributed devices (paragraph 0013)” (page 11). Paragraph [0013] of Ballard recites:

“The collection of information within network-enabled device 101 and/or dissemination of collected information by network-enabled device 101 may be in reaction to a triggering event, such as detection of an error condition. For particular types of performance data, the triggering event could be the passage of a predetermined set of time. For instance, a trigger event could be established in which performance information is collected once a month and communicated to the manufacturer's site. The performance data would preferably also include **usage data which may be used by the manufacturer to predict the life expectancy of the product** at the consumer's site, improvements **based on the consumer's use** of the product, or similar improvement. Similarly, a message sent by the manufacturer could serve as the trigger event” (emphasis added)

This section states that “usage data” is used to “predict the life expectancy of the product” and suggest “improvements based on the consumer's use of the product”. In contradiction, the Applicants’ invention uses “failure analysis data”, which is compiled based on “recovered error and other predictive statistical data” (paragraph [0025]). Ballard makes no indication of operational lifespan being devised from failure data. As such, Ballard does not disclose this element of Claim 5.

As neither Nolet nor Ballard disclose “failure analysis data provides an indication of operating lifespan”, the combination does not teach this element as well. Therefore the combination of Nolet-Ballard does not make obvious claim 5.

Furthermore, as seen above, Nolet does not disclose or suggest a “predictive failure analysis algorithm”, a server “deriving an updated predictive failure analysis algorithm”, or updating a first

microcode with a second microcode which has “different tolerances of certain error events” (e.g. in Claim 29). Assuming, that one were to combine the disclosures of Ballard and Nolet, which the Applicants do not assert there is any motivation to do so, it appears the resulting system would be that of Nolet with the ability to communicate with Simple Mail Transport Protocol. Because Ballard does not remedy the deficiency of Nolet, the combination of Nolet-Ballard does not make obvious claims 5, for at least this reason.

Claims 13 and 21 share many similarities with claim 5; therefore, many of the above arguments apply to these claims as well.

Claim 13 recites:

“The device of claim 9 wherein said **updated predictive failure analysis algorithm provides an indication of operating lifespan** of said device” (emphasis added).

Claim 21 recites:

“The method of claim 17, wherein **said updated predictive failure analysis algorithm provides an indication of operating lifespan** of said plurality of distributed devices” (emphasis added).

Consider, Claim 16, which states:

“The device of claim 15 wherein said local server includes a database arranged for storing said failure analysis data from said device, said local server being arranged for periodically uploading said failure analysis data to a manufacturer's server.”

In regards to Claim 16, the examiner states:

“Nolet teaches the device of claim 15 wherein said local server includes a database arranged for storing said failure analysis data to a server” (emphasis added).

As seen above in regards to claim 7, Nolet does not disclose or suggest a local server.

Additionally, the examiner states:

“Nolet does not explicitly teach wherein the server is a manufacturer’s server.
Ballard does teach wherein the server is a manufacturer’s server (paragraph 11).”

This section of Ballard states in part:

“Once the performance information is collected, network-enabled device 101 preferably formats the resulting data ... and the associated mail router to host computer 107 functioning as the manufacturer’s server. This communication typically occurs between two Wide Area Networks (WANs) or intranets and includes passage through one or more firewalls 104, 106 and the Internet 105. Host computer 107 preferably directs the incoming performance information to e-mail redirector and parser 108. E-mail redirector and parser 108 preferably includes programming which enables e-mail redirector and parser 108 to extract appropriate information from the incoming messages and to send those parsed portions of the incoming messages to the appropriate entities. This data, or portions thereof, may additionally or alternatively be stored in database 109.”

Figure 1 of Ballard is shown below:

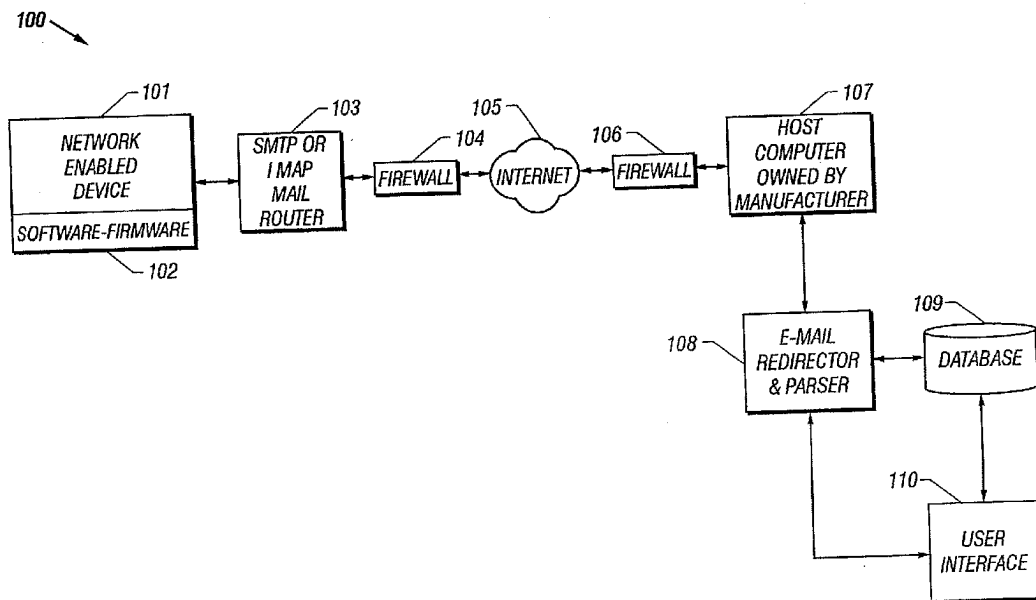


FIG. 1

As seen with Nolet, the server function, which is performed by host computer 107, is on the same side of the network as the database. This is further demonstrated by the intervening firewalls, which separate the server from the internet and the agent, and not the database. Clearly, the server in

Ballard is not a local server.

As neither Nolet nor Ballard disclose a local server, the combination does not teach this element as well. Therefore the combination of Nolet-Ballard does not make obvious claim 16.

Furthermore, as seen above, Nolet does not disclose or suggest a “predictive failure analysis algorithm”, a server “deriving an updated predictive failure analysis algorithm”, or updating a first microcode with a second microcode which has “different tolerances of certain error events” (e.g. in Claim 29). Assuming, that one were to combine the disclosures of Ballard and Nolet, which the Applicants do not assert there is any motivation to do so, it appears the resulting system would be that of Nolet with the ability to communicate with Simple Mail Transport Protocol. Because Ballard does not remedy the deficiency of Nolet, the combination of Nolet-Ballard does not make obvious claims 16, for at least this reason.

Claim 24 shares many similarities with claim 16; therefore, many of the above arguments apply to these claims as well.

Claim 24 recites:

“The method of claim 23 wherein said **local server** includes a database arranged for storing said failure analysis data, said local server being arranged for periodically uploading said failure analysis data to a manufacturer's server” (emphasis added).

Consider, Claim 26, which states:

“A server as in claim 1, wherein said network comprises a firewall, and where said failure analysis data is transmitted using a transmission protocol selected for being able to pass through said firewall.”

As seen above, Nolet does not disclose or suggest a “predictive failure analysis algorithm”, a server “deriving an updated predictive failure analysis algorithm”, or updating a first microcode with a second microcode which has “different tolerances of certain error events” (e.g. in Claim 29). Assuming, that one were to combine the disclosures of Ballard and Nolet, which the Applicants do not assert there is any motivation to do so, it appears the resulting system would be that of Nolet with the ability to communicate with Simple Mail Transport Protocol. Because Ballard does not remedy

the deficiency of Nolet, the combination of Nolet-Ballard does not make obvious claims 26, for at least this reason.

Consider, Claim 44, which states:

“A system as claim in claim 41, wherein the central server provides population statistics for distributed device ageing trends to a distributed device manufacturer for planning and budgeting considerations.”

As seen above, Nolet does not disclose or suggest a “predictive failure analysis algorithm”, a server that “modifies the predictive failure analysis algorithm”, or updating a first microcode with a second microcode which has “different tolerances of certain error events” (e.g. in Claim 41).

Likewise, Ballard does not disclose or suggest any of these elements. Consider paragraph 12 of Ballard that states: “error information collected is used to help ensure **support personnel** at the manufacturer's location can swiftly and accurately determine the underlying problem” (emphasis added). As support personnel are responsible for handling problems, it is clear that Ballard does not teach where the server “modifies the predictive failure analysis algorithm”.

Because Ballard does not remedy the deficiency of Nolet, Nolet in view of Ballard does not make obvious claims 44, for at least this reason.

In light of the discussion above, the Applicant respectfully asserts that a prima facie case for obviousness was not presented as required by the court in *In re Lee*. As such, the Applicant respectfully requests that the Examiner reconsider and withdraw these rejections.

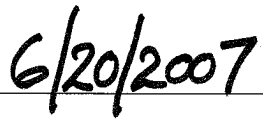
For the foregoing reasons, the Applicant believes that each and every issue raised by the Examiner has been adequately addressed and that this application has now been placed in a condition for allowance. As such, early and favorable action is respectfully solicited.

Serial No.: 10/666,970
Response to Office Action dated March 27, 2007

909B.0026.U1 (US)

Respectfully submitted:


Harry F. Smith


Date

Reg. No.: 32,493

Customer No.: 49132

HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203) 925-9400
Facsimile: (203) 944-0245
email: hsmith@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

Date

Name of Person Making Deposit